UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/876,351	06/06/2001	Doug Joseph	BEA92001008US1	9150

49474 7590 07/11/2005

LAW OFFICES OF MICHAEL DRYJA
704 228TH AVE NE
#694
SAMMAMISH, WA 98074

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/876,351	JOSEPH ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 3-8, 10-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-8 and 10-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment, and remarks therein, received on 4/11/2005 have been entered and carefully considered.
2. The Amendment introduces new limitations into the originally sole independent claims 1, 11 and 15. The newly introduced limitation has required a new search and consideration of the pending claims. The new search has resulted in newly discovered prior art. New grounds of rejection based on the newly discovered prior art follow below.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.
5. As per claims 1, 11 and 18 applicant argues that Stein does not disclose any type of secure hardware at either the first node or the second node as it is required by newly amended claims 1, 11 and 18.
6. The examiner points out that applicant does not disclose any concrete definition of the "secure hardware". The most explicit interpretation of the term is provided in the newly amended claim language, which essentially defines the secure hardware as a hardware that implements applicant's invention. As a result, the examiner considers hardware used in the invention that reads on applicant's limitations as a secure hardware.

7. Furthermore, applicant argues that processes have access to the key at the first node in *Stein*, wherein the newly added limitation prohibits all processes to access the key.

8. The examiner points out that the newly added limitation is not supported by the specification. In addition it is not clear how such a limitation would be accomplished. Besides the literal hardware keys *(e.g. a metal key to open a node's cover)* the examiner cannot foresee a key that could be used *(created, send via electronic network etc.)* without the use of computer processes. In fact the specification recites: "When a user process of a node wishes to authorize communication from another user process, it requests the kernel agent to create a channel key" *(pg. 4)*. The examiner assumes that the kernel agent is directed towards the operating system kernel process.

9. Claims 1, 3-8, 10-18 have been examined.

10. Claims 1, 3-8, 10-18 are rejected under 35 U.S.C. 101 because claims the disclosed invention is inoperative and therefore lacks utility. The invention is directed towards a secure communication involving keys, but the claim limitations prohibit all processes running on the communication platforms accessing the keys.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. Claims 1, 3-8, 10-18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.
12. The new limitation "the keys inaccessible by all processes" is not disclosed in the specification and it is not clear how such a limitation could be implemented.
13. Claims 3-8, 10, 12-14 and 16-18 are rejected by virtue of their dependence.
14. Claims 1, 3-8, 10-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
15. The following limitation: "the keys inaccessible by all processes" renders the claims indefinite because the words are not defined and are not clearly understood; as such one of ordinary skill in the art could not determine the scope of the claim. For purposes of further examination the phrase is treated as best understood.
16. Claims 3-8, 10, 12-14 and 16-18 are rejected by virtue of their dependence.

17. Claims 1, 3-7, 11, 14-16 remain rejected under 35 U.S.C. 103 (a) as being anticipated by *Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899)* in view of *Carter et al. (U.S. Patent No. 5845331).*

18. As per claim 1, as best understood, *Stein* teaches sending a key *(premaster secret),* identification of the first node, and identification of the second node from hardware of the first node *(client browser)* to hardware of the second node *(server) (pg. 41, Fig. 3.2 transaction 6, and pg. 42 first §),* receiving the key identification of the first node, and identification of the second node by the hardware of the second node and verifying the identification of the first node *(pg. 41, Fig. 3.2, transaction 7, pg.42 second §)* and the identification of the second node at the hardware of the second node , and storing the key at the hardware of the second node *(pg. 42 first §).* Once an SSL connection is in place the secure hardware of the first hardware and the secure hardware of the second node establish a channel over which the process of the first node and the process of the second node are able to communicate *(SSL Characteristics, in particular pg. 40).*

19. Each layer in TCP/IP *(or any other OSI "compatible" architecture)* has different responsibilities and processes at each layer carrying these responsibilities have different functions. In the *Stein's* teaching the *SSL* communication is invoked by web browser/server interaction and all processes invoking *SSL* mechanism have no access to keys, which are produced and used at SSL level.

20. *Stein* does not explicitly teach that unauthorized processes running on the first node are unable to send unauthorized messages.

21. *Carter et al.* teach to preventing unauthorized processes to conduct unauthorized activities *(col. 1 lines 24-35)*, which reads on preventing unauthorized processes to unable to send unauthorized messages.

22. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages. One of ordinary skill in the art would have been motivated to perform such a modification in order to secure sending messages to only authorized processes.

23. Claims 11 and 15 are substantially equivalent to claim 1; therefore claims 11 and 15 are similarly rejected.

24. As per claims 5 and 6 TCP/IP includes source and destination ports.

25. As per claim 10 processing the message at the process of the first node upon successful verification of the key at the secure hardware of the first node is implicit.

26. Claims 1, 3-7, 11, 14-16 remain rejected under 35 U.S.C. 103 (a) as being anticipated by *Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899)* in view of *Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00)*.

27. As per claim 1, as best understood, *Stein* teaches sending a key *(premaster secret)*, identification of the first node, and identification of the second node from hardware of the first node *(client browser)* to hardware of the second node *(server) (pg. 41, Fig. 3.2 transaction 6, and pg. 42 first §)*, receiving the key identification of the first node, and identification of the second node by the hardware of the second node and verifying the identification of the first node *(pg. 41, Fig. 3.2, transaction 7, pg.42 second §)* and the identification of the second node at the hardware of the second

node , and storing the key at the hardware of the second node *(pg. 42 first §)*. Once an SSL connection is in place the secure hardware of the first hardware and the secure hardware of the second node establish a channel over which the process of the first node and the process of the second node are able to communicate *(SSL Characteristics, in particular pg. 40)*.

28. Each layer in TCP/IP *(or any other OSI "compatible" architecture)* has different responsibilities and processes at each layer carrying these responsibilities have different functions. In the *Stein's* teaching the *SSL* communication is invoked by web browser/server interaction and all processes invoking *SSL* mechanism have no access to keys, which are produced and used at SSL level.

29. *Stein* does not explicitly teach that unauthorized processes running on the first node are unable to send unauthorized messages.

Fontana teaches Microsoft Outlook E-mail security patch that prevents unauthorized processes from sending unauthorized messages *(Fontana, pg. 2)*. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages as taught by *Fontana*. One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent worms from spreading to other nodes.

30. Claims 11 and 15 are substantially equivalent to claim 1; therefore claims 11 and 15 are similarly rejected.

31. As per claims 5 and 6 TCP/IP includes source and destination ports.

32. As per claim 10 processing the message at the process of the first node upon successful verification of the key at the secure hardware of the first node is implicit.

33. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899)* in view of *Carter et al. (U.S. Patent No. 5845331)* and in further view of *Ogawa et al. (U.S. Patent No. 5802065).*

34. *Stein* in view of *Carter et al.* teach verifying the identification of the first node and the identification of the second node at the hardware of the second node as discussed above. *Stein* in view of *Carter et al.* do not explicitly teach verifying the identification of the first node and the identification of the second node at the hardware of the second node comprising verifying the identification of the first node and the identification of the second node in a channel state table accessible by the hardware of the second node and accessible by all the processes of the second node. Ogawa et al. teach verifying the identification of one node and the identification of another node in a channel state table accessible by the hardware of the one node and accessible by all of the processes of the one node *(Ogawa et al. col. 4 lines 50-56 and col. 5 lines 4-11).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to verify the identification of the first node and the identification of the second node in a channel state table accessible by the hardware of the second node and accessible by all the processes of the second node as taught by Ogawa. One of ordinary skill in the art would have been motivated to perform such a modification in order to enhance security and operation speed.

35. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899)* in view of *Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00)* and in further view of *Ogawa et al. (U.S. Patent No. 5802065).*

36. *Stein* in view of *Fontana* teach verifying the identification of the first node and the identification of the second node at the hardware of the second node as discussed above. *Stein* in view of *Fontana* do not explicitly teach verifying the identification of the first node and the identification of the second node at the hardware of the second node comprising verifying the identification of the first node and the identification of the second node in a channel state table accessible by the hardware of the second node and accessible by all processes of the second node. Ogawa et al. teach verifying the identification of one node and the identification of another node in a channel state table accessible by the hardware of the one node and accessible by all processes of the one node *(Ogawa et al. col. 4 lines 50-56 and col. 5 lines 4-11).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to verify the identification of the first node and the identification of the second node in a channel state table accessible by the hardware of the second node and accessible by all the processes of the second node as taught by Ogawa. One of ordinary skill in the art would have been motivated to perform such a modification in order to enhance security and operation speed.

37. Claim 16 remains rejected under 35 U.S.C. 103(a) as being unpatentable over *Stein (U.S. Pub. No. 20020087884)* in view of in view of *Carter et al. (U.S. Patent No. 5845331)* and in further view of *Baker et al. (U.S. Patent No. 6611498).*

38. *Stein* in view of *Carter et al.* teach storing the key at the hardware of the second node as discussed above. *Stein* in view of *Carter et al.* do not teach storing the key comprising storing the key in a key table. *Baker et al.* teach storing the key comprising storing the key in a key table *(Baker et al., col. 17 lines 4-18).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to store the key in the key table as taught by *Baker et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to map keys to the associated session.

39. Claims 12-13 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Stein (U.S. Pub. No. 20020087884)* in view of *Carter et al. (U.S. Patent No. 5845331)*, *Baker et al. (U.S. Patent No. 6611498)* and *Ogawa et al. (U.S. Patent No. 5802065)* and in further view of *Bean et al. (U.S. Patent No.4843541).*

40. *Stein* in view of *Carter et al.*, *Baker et al.* and *Ogawa et al.* teach a first and a second key table and first and second connection tables as discussed above. *Stein* in view of *Carter et al.*, *Baker et al.* and *Ogawa et al.* do not explicitly teach node entries identifying one of the one or more partitions in which processes are running on the nodes. *Bean et al.* teach unique partition identifiers identifying nodes partitions *(col. 50 lines 55-66).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include partition identifiers as taught by *Bean et al.*

within the first and second connection tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to extend the security enhancement and operation speed to systems wherein plurality of different preferred guest programming systems could run simultaneously in the different partitions.

41. Claims 12-13 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Stein (U.S. Pub. No. 20020087884)* in view of *Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00)*, *Baker et al. (U.S. Patent No. 6611498)* and *Ogawa et al. (U.S. Patent No. 5802065)* and in further view of *Bean et al. (U.S. Patent No.4843541).*

42. *Stein* in view of *Fontana*, *Baker et al.* and *Ogawa et al.* teach a first and a second key table and first and second connection tables as discussed above. *Stein* in view of *Fontana, Baker et al.* and *Ogawa et al.* do not explicitly teach node entries identifying one of the one or more partitions in which processes are running on the nodes. *Bean et al.* teach unique partition identifiers identifying nodes partitions *(col. 50 lines 55-66).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include partition identifiers as taught by *Bean et al.* within the first and second connection tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to extend the security enhancement and operation speed to systems wherein plurality of different preferred guest programming systems could run simultaneously in the different partitions.

43. Claims 1 and 10 remain rejected under 35 U.S.C. 103(a) as being anticipated by *Win et al. (U.S. Patent No. 6161139)* in view of *Carter et al. (U.S. Patent No. 5845331)*.

44. As per claim 1, *Win et al.* teach sending a key *(cookie)* from hardware of the first node *(web server)* to hardware of the second node *(client's web browser)* which is stored at the hardware of the second node *(col. 6 lines 25-29)*. The application uses TCP/IP and as a result the first node and the second node verifies first node and second node identification.

45. As per claim 10, *Win et al.* teach the second node sending the key and the message to the first node, which verifies the key and processes the message *(URL, col. 6 lines 29-33 and 37-44)*.

46. *Win et al.* do not explicitly teach that unauthorized processes running on the first node are unable to send unauthorized messages. *Carter et al.* teach to preventing unauthorized processes to conduct unauthorized activities *(col. 1 lines 24-35)*, which reads on preventing unauthorized processes to unable to send unauthorized messages. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages. One of ordinary skill in the art would have been motivated to perform such a modification in order to secure sending messages to only authorized processes.

47. Claims 1 and 10 remain rejected under 35 U.S.C. 103(a) as being anticipated by *Win et al. (U.S. Patent No. 6161139) Fontana (John Fontana, Defending against*

Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00).

48. As per claim 1, *Win et al.* teach sending a key *(cookie)* from hardware of the first node *(web server)* to hardware of the second node *(client's web browser)* which is stored at the hardware of the second node *(col. 6 lines 25-29).* The application uses TCP/IP and as a result the first node and the second node verifies first node and second node identification.

49. As per claim 10, *Win et al.* teach the second node sending the key and the message to the first node, which verifies the key and processes the message *(URL, col. 6 lines 29-33 and 37-44).*

50. *Win et al.* do not explicitly teach that unauthorized processes running on the first node are unable to send unauthorized messages. *Fontana* teaches Microsoft Outlook E-mail security patch that prevents unauthorized processes from sending unauthorized messages *(Fontana, pg. 2).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages as taught by *Fontana.* One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent worms from spreading to other nodes.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

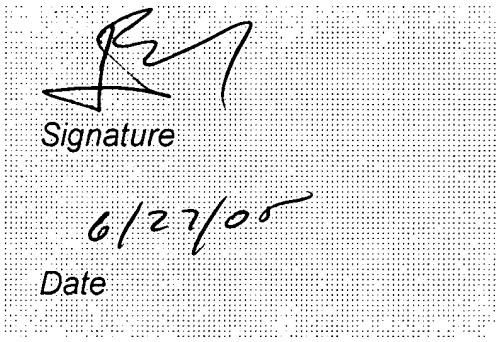
§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



David Y. Jung
Primary Examiner

6/25/05